

UNITED STATES DISTRICT COURT

for the
Southern District of OhioIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Samsung Galaxy A53 cell phone bearing serial number
R5CTA1S8KJR belonging to and seized from John
Sullivan

Case No. 2:23-mj-389

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment B incorporated herein by reference

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See attachment A incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Sections 2252 and 2252(a)2	Distribution/Receipt/Possession/Accessing with Intent to View of Child Pornography/Visual Depictions of Minors Engaged in Sexually Explicit Conduct in Interstate Commerce

The application is based on these facts:

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

TFO Brett M. Peachey

Printed name and title

Sworn to before me and signed in my presence.

Date: 6/27/2023

City and state: Columbus OH

Chelsey M. Vascara
United States Magistrate Judge

Judge's signature

Chelsey M. Vascara-United States Magistrate Judge

Printed name and title



**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT, EASTERN DIVISION OF OHIO**

In the Matter of the Search of:)	
)	Case No.: 2:23-mj-389
Samsung Galaxy A53 cell phone with serial number)	
R5CTA1S8KJR belonging to John Sullivan)	
recovered from his person and currently held at FBI)	
Columbus Resident Agency 425 W. Nationwide Blvd.)	Magistrate Judge Vascura
Columbus, OH 43215)	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brett M. Peachey, a Task Force Officer with the Federal Bureau of Investigation (FBI),
being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I have been employed as a police officer with the City of Westerville since December of 1995. In March of 2008, I began as a Task Force Officer for the FBI, and am currently assigned to the Child Exploitation Task and Human Trafficking Task Force, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children including the online exploitation of children.

2. During my career as a police and task force officer, I have participated in various investigations of computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a police and task force officer, I investigate criminal violations relating to child exploitation and child pornography including the online enticement of minors and the illegal distribution, transmission, receipt, possession, and production of child pornography, in violation of 18 U.S.C. §§ 2252(a), 2252A, 2251 and 2422.

3. As a task force officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other subjects and witnesses. I have not included in this affidavit all information known by me relating to the investigation. I have only set forth facts believed to be necessary to establish probable cause in support of a search warrant for the following digital media; Samsung Galaxy A-53 cell phone with serial number R5CTA1S8KJR seized from John Sullivan while a resident of Alvis House Community Residential Reentry Center 1755 Alum Creek Drive Columbus, OH 43207 on or about June 17, 2023 (hereinafter referred to as "the SUBJECT MEDIA"). The SUBJECT MEDIA was seized pursuant to a violation of Sullivan's community based program release from prison. I have not withheld any evidence or information that would negate probable cause.

5. The SUBJECT MEDIA to be searched is more particularly described in Attachment B, for the items specified in Attachment A, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, – the advertising, distribution, transmission, receipt, and/or possession of child pornography.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.

7. Title 18 United States Code § 2252 makes it a crime to knowingly transport, ship, receive, distribute, sell or possess in interstate commerce any visual depiction involving the use of a minor engaging in sexually explicit conduct.

8. Title 18 United States Code § 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate commerce.

9. The term "child pornography"¹, as used herein, is defined pursuant to Title 18, United States Code, Section 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of

¹ 1 The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually conduct.”

10. The term "sexually explicit conduct", as used in 18 U.S.C. Section 2252, is defined pursuant to Title 18, United States Code, Section 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." Pursuant to Title 18, United States Code, Section 2256(2)(B), "sexually explicit conduct" when used to define the term child pornography, also means "(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.”

11. "Minor" as used herein is defined pursuant to 18 U.S.C. § 2256(1) as any person under the age of eighteen years.

12. The term "visual depiction", as used herein, is defined pursuant to Title 18, United States Code, Section 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."

13. "Graphic" when used with respect to a depiction of sexually explicit conduct, means that the viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10)).

14. Pursuant to Title 18, United States Code, Section 1591(e)(3) the term "commercial sex act" is defined as "any sex act, on account of which anything of value is given to or received by any person.”

15. Pursuant to Title 18, United States Code, Section 2256(1), the word "minor" means any person under the age of eighteen years.

16. The term "computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. . . ." (18 U.S.C. §§ 1030(e)(1) and 2256(6)).

IV. BACKGROUND REGARDING COMPUTERS, CELL PHONES AND DIGITAL STORAGE DEVICES

17. Based on my training and experience, I use the following terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile/cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, modern wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital image files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. This storage media can contain any digital data, including data unrelated to photographs or videos. Most digital cameras also include a screen for viewing the stored images.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

18. Based on my training, experience, and observation of the device, I know that the SUBJECT DEVICE has abilities that allow it to serve as a mini handheld computer, electronic storage device, wireless telephone, digital camera, digital video recorder, portable media player, GPS navigation device, and to connect to the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, where the device has been, and what messages were

sent to or from the device via text message, e-mail, or other internet-based messaging applications.

19. I know from my training and experience that computer hardware, software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of the crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, instrumentalities of a crime and/or fruits of a crime.

20. Digital or electronic files or remnants of such files can be recovered months or even years after they have been saved on a hard drive or other digital device, deleted, or viewed via the Internet, and can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of storage space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

21. Computers, tablets and smart/cellular phones are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including AGIF@ (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

22. Computers, tablets and smart/cellular phones are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

23. The Internet is a worldwide network of computer systems operated by governmental

entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers or cellular network; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP.

24. Computers and mobile computing devices have the capability to store data in digital form. Cellular “smart” phones are essentially mini computers that can store anywhere from 32GB to 256GB of data. These phones have the capability to store hundreds of thousands of pieces of information which includes various forms of communication via various applications and text messaging. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

25. Searches and seizures of evidence from computers and mobile computing devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (like hard drives, USB or “thumb” drives, SD cards, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored; and
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

26. In order to fully retrieve data from a computer system, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

VI. SEARCH METHODOLOGY TO BE EMPLOYED

27. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in Attachment A;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the items listed in Attachment A;
- c. surveying various files, directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

VII. INVESTIGATION AND PROBABLE CAUSE`

28. On April 11, 2012, John Sullivan pleaded guilty to one count of Possessing Visual Depictions of Child Pornography in Interstate Commerce in U.S. District Court in Columbus, OH and sentenced to 30 months imprisonment. After being released, Sullivan was again charged with Possessing Visual Depictions of Child Pornography in Interstate Commerce, plead guilty on April 15, 2015 and sentenced to an additional 121 months imprisonment.

29. On April 27, 2023, Sullivan was released from his second conviction and transferred from FCI Elkton to the Alvis House Residential Reentry Center located at 1755 Alum Creek Drive Columbus, OH 43215. Upon his arrival at Alvis House, Sullivan signed orientation and intake paperwork agreeing to follow the rules and regulations of the Residential Reentry Center. In addition, he signed the Community Based Program Agreement which, in part, states that he understands that he is required to abide by condition of supervision as imposed by the sentencing court.

30. On June 17, 2023, an employee of Alvis House entered Sullivan's room and noticed that Sullivan appeared to be attempting to conceal his phone. Due to this suspicious behavior the employee seized Sullivan's phone and conducted a search of it which is permissible within the

policies of Alvis House. The employee observed several social media apps which included conversations with females and animated pictures of nude underage females which is a violation of the center's rules and regulations. The phone was turned over to Christina Simpson who is the Federal Program Manager of the center. Simpson continued to search Sullivan's phone and observed numerous photos of prepubescent females lasciviously displaying their genitals and engaged in sexual activity.

31. The Columbus Police Department was notified and an officer arrived at the scene and completed a miscellaneous report at that time to document the incident.

32. After being advised of the contraband observed on Sullivan's phone, Michael Staruk of the Bureau of Prisons contacted the United States Attorney's Office in Columbus who, in turn, contacted your affiant to conduct an investigation.

33. On June 23, 2023, your affiant travelled to Alvis House and took possession of the phone from Christina Simpson. The phone is currently being maintained in secure storage at the FBI Columbus Resident Agency 425 W. Nationwide Blvd, Columbus, OH 43215.

34. Based on the above information, your affiant believes that evidence of the receipt, possession and distribution of child pornography is present on the SUBJECT MEDIA.

VIII. CHARACTERISTICS COMMON TO THOSE WITH A SEXUAL INTEREST IN CHILDREN

35. Based on my own knowledge, experience, and training in online child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in minors and/or seek to sexually exploit minors via online communications:

A. Those who have a sexual interest in minors, may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from discussions of or literature describing such activity.

B. Those who have a sexual interest in children and/or seek to sexually exploit minors via online communications may collect sexually explicit or suggestive materials in a variety of media. These materials are frequently used for the sexual arousal and gratification of the individual. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

C. Individuals who have a sexual interest in children have been found to: download, view, then delete child pornography on a cyclical and repetitive basis; view child

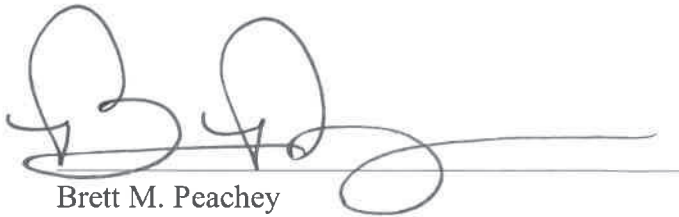
pornography without downloading or saving it; or save child pornography materials to cloud storage. Traces of such activity can often be found on such individual's computers or digital devices, for months or even years after any downloaded files have been deleted.

D. Those who have a sexual interest in minors may correspond online with and/or meet others to share information about how to find child victims, exchange stories about their sexual exploits with children, and/or exchange child pornography materials; and tend to conceal and maintain in a safe, secure and private environment such correspondence as they do any sexually explicit material related to their illicit sexual interest.

E. When communications relating to a sexual interest in children, and/or child pornography files are stored on or accessed by computers and related digital media, forensic evidence of the accessing, downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such files have been deleted from the computers or digital media.


IX. CONCLUSION

36. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2252(a), 2252A, 2251 and 2422 have been committed, and evidence of those violations is located in the SUBJECT MEDIA described in Attachment B. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment A.

A handwritten signature in black ink, appearing to read "Brett M. Peachey", written over a horizontal line.

Brett M. Peachey
Task Force Officer
Federal Bureau of Investigation

Sworn to and subscribed before me this 27th day of June 2023.

A handwritten signature in blue ink, appearing to read "Chelsey M. Vascara", written over a horizontal line.

Chelsey M. Vascara
United States Magistrate Judge
United States District Court
Southern District of Ohio

ATTACHMENT A
LIST OF ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252 and 2252(a)(2).

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, communications or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, letters, e-mail messages, chat logs, text or other electronic messages, other digital data files and web cache information) pertaining to the possession, receipt, advertising for, or distribution of child pornography, or the online solicitation or enticement of minors for purposes of commercial or other illegal sexual activity.
3. In any format and medium, all originals, computer files, copies, and negatives of child pornography or child erotica.
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, e-mail messages, chat logs and text or other electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography.
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, text or other electronic messages, and other digital data files) concerning communications between John Sullivan and any other individuals related to the sexual abuse or exploitation (commercial or otherwise) of minors.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, e-mail messages, chat logs, text or other electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child

pornography or that cater to those with a sexual interest in children.

7. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
8. Any and all visual depictions of minors, whether clothed or not, for comparison to and identification of any child pornography images or videos discovered.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography or visual depictions of minors engaged in sexually explicit conduct to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, letters, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
11. Any and all digital diaries, notebooks, notes, and any other records reflecting personal contact, sexual activity, and/or any other activities with minors visually depicted while engaged in sexually explicit conduct.

ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEARCHED

- 1) Samsung Galaxy A53 cell phone with serial number R5CTA1S8KJR

The above item was seized during Sullivan's residency at the Alvis House Community Residential Reentry Center 1755 Alum Creek Drive Columbus, OH 43207 and turned over to your affiant by an employee of the center on June 23, 2023. It is currently being held in FBI Columbus secure storage located at 425 W. Nationwide Blvd, Columbus Ohio, 43215.